Fake Social Security Statement emails trick users into installing remote tool

By Pieter Arntz

Published: 2025-04-30 · Archived: 2026-04-05 14:34:49 UTC

Fake emails pretending to come from the US Social Security Administration (SSA) try to get targets to install ScreenConnect, a remote access tool.

This campaign was flagged and investigated by the Malwarebytes Customer Support and Research teams.

ScreenConnect, formerly known as ConnectWise Control, is a remote support and remote access platform widely used by businesses to facilitate IT support and troubleshooting. It allows technicians to remotely connect to users' computers to perform tasks such as software installation, system configuration, and to resolve issues.

Because ScreenConnect provides full remote control capabilities, an unauthorized user with access can operate your computer as if they were physically present. This includes running scripts, executing commands, transferring files, and even installing malware—all potentially without you realizing.

This makes ScreenConnect a dangerous tool in the hands of cybercriminals. A phishing group dubbed Molatori—because of the domains they use to host the ScreenConnect client—has been found to lure their targets into installing the ScreenConnect clients by sending emails pretending to come from the Social Security Administration (SSA):

> "Your Social Security Statement is now available
> Thank you for choosing to receive your statements electronically.
> Your document is now ready for download:
>
> - Please download the attachment and follow the provided instructions.
> - NOTE: Statements & Documents are only compatible with PC/Windows systems."

There are some variations to this mail in circulation but the example above shows how legitimate these emails look.

The link in the email leads to the ScreenConnect support.Client.exe, but was found under several misleading names like `ReceiptApirl2025Pdfc.exe`, and `SSAstatment11April.exe`.

After cybercriminals install the client on the target's computer, they remotely connect to it and immediately begin their malicious activities. They access and exfiltrate sensitive information such as banking details, personal identification numbers, and confidential files. This stolen data can then be used to commit identity theft, financial fraud, and other harmful acts. Experts have identified financial fraud as the primary objective of the Molatori group.

There are several circumstances that make this campaign hard to detect:

- The cybercriminals send phishing emails from compromised WordPress sites, so the domains themselves appear legitimate and not malicious.
- They often embed the email content as an image, which prevents email filters from effectively scanning and blocking the message.
- ScreenConnect is a legitimate application which happens to be abused because of its capabilities.

What we can do

When receiving unsolicited emails there are a few necessary precautions you can take to avoid falling for phishing:

- Verify the source of the email through independent sources.
- Don't click on links until you are sure they are non-malicous.
- Don't open downloaded files or attachments until you are sure they are safe.
- Use an up-to-date and active anti-malware solution.
- If you suspect an email isn't legitimate, take a name or some text from the message and put it into a search engine to see if any known phishing attacks exist using the same methods.

Malwarebytes users are protected

Malwarebytes will detect suspicious instances of the ScreenConnect client as RiskWare.ConnectWise.CST.

And blocks connections to these associated domains:

- atmolatori[.]icu
- gomolatori[.]cyou
- molatoriby[.]cyou
- molatorier[.]cyou
- molatorier[.]icu

- molatoriist[.]cyou
- molatorila[.]cyou
- molatoriora[.]cyou
- molatoriora[.]icu
- molatoripro[.]cyou
- molatoripro[.]icu
- molatorisy[.]cyou
- molatorisy[.]icu
- onmolatori[.]icu
- promolatori[.]icu
- samolatori[.]cyou
- samolatori[.]icu
- umolatori[.]icu

About the author

Was a Microsoft MVP in consumer security for 12 years running. Can speak four languages. Smells of rich mahogany and leather-bound books.
